

REMARKS

The Applicants request reconsideration of the rejection.

Claims 26-29 are now canceled in favor of new claims 30 and 31. Thus, the outstanding rejections are moot; the Applicants make no admission as to their propriety. However, the Applicants note that new claims 30-31 are distinguishable from the two documents cited against canceled claims 26-29 (Belani, et al., US 6,772,350 (Belani) in view of Chang, et al., US 2003/0229623 (Chang)) as follows.

New claim 30 feature "hierarchical access permission setting values", established with respect to access operations having different priority levels predefined for "identification information" of a user terminal and for "communication capability information" of the user terminal. The access operations include, for example, information disclosure, information read and information write as described by referring to FIG. 5 and the associated disclosure. These terms have been discussed in previous papers submitted in the prosecution history of this application.

The communication capability information may include, for example, the various types of information items 42-46 as shown in FIG. 5.

The emphasis of the present claims is on how to update the hierarchical access permission setting values.

According to the present claims, when a request is received for changing the access permission setting value of a specific one of the access operations for the communication capability information from a non-permission state to a permission state, a controller operates so as to rewrite the access permission values of access operations which each have a priority level equal to or higher than that of the specific

access operation into the permission state in both the identification information and the communication capability information.

In turn, when a request is received for changing the access permission setting value of a specific access operation for the identification information from the permission state to the non-permission state, the controller operates so as to rewrite access permission values of access operations which each have a priority level equal to or higher than that of the specific access operation into the non-permission state, also in both the identification information and the communication capability information.

Belani proposes a system for controlling access to resources, which uses "an access information list" for indicating, in association with each resource as shown in FIG. 3, users who are allowed to access the resources, and operations authorized for each user to perform on the resources. Belani also appears to disclose "user hierarchy information" for indicating one or more groups to which a user belongs, and "resource hierarchy information." With regard to the resource hierarchy information, Belani appears to disclose that a resource "R4", which is a descendant of a resource "R2", inherits both the access list information of resources "R2" and "R1" because resource "R2" inherits the access list information of resource "R1."

Although Belani permits each user to perform specific operations on specific resources by using the access information list and the resource hierarchy information, Belani's access control is carried out based on an access information list having fixed contents, and based on resource hierarchy information indicating a hierarchical relation among resources that have the same access information list. Belani does not describe about how to update the fixed contents of the access

information list, and thus does not disclose or fairly suggest a controller that operates, in response to a request for changing the access permission setting value of a specific access operation for communication capability information from a non-permission state to a permission state (or from a permission state to a non-permission state), so as to rewrite access permission values of access operations each having a priority level equal to or higher than that of the specific access operation in both the identification information and the communication capability information.

By way of illustrative example, the Applicants direct the Examiner to FIGS. 18 and 30 of the present application, wherein the access permission setting values of the identification information (3111) and the access permission setting values of the communication capability information (3112-3117) are shown, and do not correspond to the inheritance relationship disclosed as Belani's resource hierarchy information.

The secondary reference to Chang appears is directed to security authorization of networked computer resources, and seems to suggest assignment to each user of a role and a level of access within a hierarchically organized system of resources (system objects) such as domains, clusters, and application servers. However, Chang fails to teach the hierarchical access permission setting values and a controller that operates, in response to a request for changing the access permission setting value of a specific access operation for communication capability information from a non-permission state to a permission state (or from a permission state to a non-permission state), so as to rewrite access permission values of access operations each having a priority level equal to or higher than that of the specific

access operation in both the identification information and the communication capability information.

Because neither Belani nor Chang discloses the above-claimed features in independent claim 30, it necessarily follows that any combination of their teachings also fails to suggest these features. Furthermore, although no argument as to the separate patentability of dependent claim 31 is advanced in this paper, for brevity, claim 31 inherits the patentable features of claim 30 as argued above, and thus is also patentable. Accordingly, claims 30-31 are patentable over Belani in view of Chang or any other reference of record.

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Brundidge & Stanger, P.C., Deposit Account No. 50-4888 (referencing attorney docket no. NIT-415).

Respectfully submitted,

BRUNDIDGE & STANGER, P.C.

/Daniel J. Stanger/
Daniel J. Stanger
Registration No. 32,846

DJS/kah
(703) 684-1470